

REMARKS

Applicants have now had an opportunity to carefully consider the Examiner's comments set forth in the Final Office Action of April 14, 2004.

All of the Examiner's objections and rejections are traversed.

Reexamination and reconsideration are respectfully requested.

The Office Action

Claims 1 and 3-7 remain in this application. Claim 2 has been cancelled, and claim 1 has been amended to incorporate the features of claim 2.

Claims 1-4, 6 and 7 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Haber (U.S. Patent N. 5,136,147) in view of Doyle (U.S. Patent No. 6,381,696) and further in view of Romney (U.S. Patent No. 6,085,322).

Claim 5 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Haber in view of Doyle and further in view of Labozzeta (U.S. Patent No. 5,107,269).

Claims 1 and 3-7 are distinguished from the cited art.

Claims 1 and 3-7 Are Distinguished From The Cited Art

The present application teaches a novel method for securing the integrity of files prior to archiving and involves an exchange between a client and a Time Source Provider (a trusted third party). In particular, as illustrated in amended claim 1, the client's Public and Private Key pair are organizationally associated. In other words, the key pair is associated with an organization/corporate unit, or individual. (See page 6, lines 2-3 of the Specification.) If the key pair is reserved for archiving then the risk of exposure and compromising is decreased. None of the cited references disclose this feature.

Initially, it is noted that the Examiner has cited Romney in connection with original claim 2. However, it is believed that the Examiner intended to cite Doyle. Doyle relates to the digital time stamping of data, without the need for subsequent third party verification, by the chaining of key pairs, the key pairs being generated for particular time intervals. Doyle, does not, however, teach or suggest the concepts of the present application, such as generating a Public and Private Key pair for both the client and the Time Source Provider and then using

the Key pairs to encrypt and decrypt the files.

In column 5, lines 34-39, Doyle discloses:

In step 2010 a key pair is generated. As is known in the art, the key pair includes a public key and a private key. According to an embodiment of the present invention, a key pair is generated for each time interval utilized by the system implementing the time stamping method. The implementing system can include, for example, a conventional general purpose computer, such as a microprocessor based personal computer or server. In an embodiment of the present invention, the method is implemented in software that executes on a client-server computer system architecture. The time interval can be any defined period, e.g., every second, 10 seconds, minute or 10 minutes. The current time interval is referred to as t_n and the next time interval is referred to as t_{n+1} . For the purposes of time stamping documents, accuracy to the minute may be sufficient for subsequent authentication purposes.

Yet Doyle fails to teach or suggest that the public and private key pair is "organizationally associated" as provided in amended claim 1. Rather, Doyle discloses that:

key pairs are generated for particular time intervals and time stamp requests are automatically carried out using the private key for the time interval, the private key being destroyed after the time interval. In another embodiment of the present invention, the private key of a prior time interval is used to sign the public key for a subsequent time interval before the private key of the prior time interval is destroyed. In this embodiment of the present invention, every time interval has its own key pair for which the private key is destroyed after signing the public key for the next time interval. According to the present invention, key pairs do not have to be continuously generated every time interval, but can be pre-generated and selected from a queue for each time interval that a time stamp request is received.

Accordingly, claim 1, as amended, and claims 3-7, which depend therefrom, are distinguishable from the cited art.

Applicant further submits that claim 5, which includes the "application of multiple or differing error correcting codes to the representation of time, the time source calibration data, the file attributes and the encryption key signatures," is patentably distinguishable from the cited art. As noted by the Examiner, Haber and Doyle fail to teach this feature. The other cited reference, Labozzetta, relates to a device used in monopulse radar systems for correcting the differential error contained in the raw Off-Boresight Angle value obtained in such systems, especially when used for azimuth tracking, *i.e.*, it is a differential error correction device. As

disclosed in Labozzetta in column 4, lines 5-20:

The statistical averaging and linearization performed in the feedback loop 22 substantially eliminates deterministic errors commonly found in systems used for differential error correction in monopulse receivers known presently in the art, an example of which is shown in FIG. 2. Such deterministic errors are commonly caused by variations of system tolerances and the effects of those tolerances on the antenna construction and design, as well as periodic time variations and thermal variations of the system, which could occur and produce errors in the same direction of the angular origin of the received radar signals. These deterministic errors, which produce inaccurate OBA detection in currently known differential error correction systems, are substantially eliminated through the use of the inventive feedback loop previously described.

Thus, Labozzetta does not in any way teach or suggest *applying multiple or differing error correcting codes to the representation of time, the time source calibration data, the file attributes and the encryption key signatures*. Accordingly, claim 5 is patentably distinguishable over the cited art.

CONCLUSION

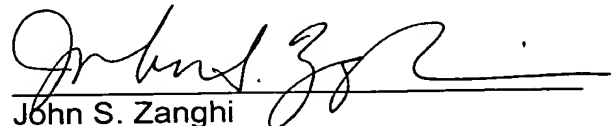
For the reasons detailed above, it is submitted all claims remaining in the application (Claims 1 and 3-7) are now in condition for allowance. The foregoing comments do not require unnecessary additional search or examination.

No additional fee is believed to be required for this Amendment After Final. However, the undersigned attorney of record hereby authorizes the charging of any necessary fees, other than the issue fee, to Xerox Deposit Account No. 24-0037.

In the event the Examiner considers personal contact advantageous to the disposition of this case, he/she is hereby authorized to call John S. Zanghi, at Telephone Number (216) 861-5582.

Respectfully submitted,

FAY, SHARPE, FAGAN,
MINNICH & McKEE, LLP



John S. Zanghi
Reg. No. 48,843
1100 Superior Avenue, 7th Floor
Cleveland, Ohio 44114-2579
(216) 861-5582

Date

7/14/04